1.   A method for providing security with respect to who provided digital data at what time, said method comprising the steps of:

performing a serially chained certification process including:

(a) forming a first interval certification at a first server including the server's identification, the start time of an interval chain in UTC, the start time of the interval in UTC, the stop time of the interval, a public key for the interval, a digital signature for the interval, signed by a previous interval's private key, and a digital signature for the interval, signed by the interval's private key;

(b) upon expiration of the first interval, destroying its private key;

(c) configuring a second server to request a cross-certification for a second interval so that the first server is effectively requested to provide independent proof of the existence of the interval (and its public key) at a point in time witnessed by the first server;

(d) continuing steps (a), (b), and (c) for second, third, and following intervals so that intervals are cross-chained with other servers to form a widely witnessed, temporal web of signed intervals of time.